Theoretical Computer Science 94 (1992) 367–371
Elsevier

A note on renewal systems

Antonio Restivo

Dipartimento di Matematica e Applicazioni, Università di Palermo, Via Archirafi 34, 90123 Palermo, Italy

Abstract

Restivo, A., A note on renewal systems, Theoretical Computer Science 94 (1992) 367–371.

A renewal system is a symbolic dynamical system generated by free concatenations of a finite set of words. In this paper we prove that, given two systems which are both renewal and Markov systems, it is decidable whether they are topologically conjugate. The proof makes use of the methods and the techniques of formal language theory.

Let A be a finite alphabet. Denote by A^Z the set of all bi-infinite sequences of the elements of A. Let us endow A with the discrete topology and A^Z with the product topology. Then A^Z is a compact space. The *shift* is the mapping $\sigma: A^Z \to A^Z$ defined by $\sigma((a_n)_{n\in Z}) = (a_{n+1})_{n\in Z}$. The shift is a homeomorphism of A^Z. A *symbolic dynamical system* is a closed subset S of A^Z which is invariant under σ.

Let A^* denote the set of all finite sequences (the "words") of the elements of A endowed with the usual concatenation product. A^* is the free monoid generated by A. A subset L of A^* is *factorial* if every factor of elements of L is an element of L: $uv \in L$ implies that $u \in L$ and $v \in L$. L is *extensible* if every element of L is extensible: for every $w \in L$, there exist $a, b \in A$ such that $awb \in L$.

If S is a subset of A^Z, for any $s = (a_n)_{n\in Z} \in S$ and for any pair of integers $i \leqslant j$, denote by $s(i, j)$ the word $a_i a_{i+1} \ldots a_j$ of A^*. A symbolic dynamical system $S \subseteq A^Z$ is uniquely specified (cf. [6]) by the associated subset $L(S)$ of A^*:

$$L(S) = \{s(i, j) \in A^* \mid s \in S,\ i \leqslant j\}.$$

By definition, $L(S)$ is factorial and extensible.

If L is a factorial subset of A^*, then it is the complement of an ideal of A^*, i.e. $L = A^* - A^* H A^*$. $S \subseteq A^Z$ is a *system of finite type* if $L(S)$ is the complement of a finitely generated ideal of A^*: $L(S) = A^* - A^* H A^*$, with H a finite subset of A^*. S is then defined by specifying a finite set H of forbidden words which do not occur anywhere

as factors in the words of $L(S)$. If $H \subseteq A^2$, we say that S is a *Markov system*. A Markov system can be described by a directed graph whose nodes are the elements of A and whose edges are the elements of $A^2 - H$ (the transitions).

$S \subseteq A^Z$ is a *sofic system* [10] if $L(S)$ is a *rational* (see [7]) subset of A^*. S is then defined by specifying a finite automaton recognizing $L(S)$. In particular, a system of finite type is a sofic system.

A system $S \subseteq A^Z$ is *transitive* if, for all $u, v \in L(S)$, there exists $w \in A^*$ such that $uwv \in L(S)$.

Let X be a subset of A^*. Let us denote by X^* the submonoid of A^* generated by X, and by $F(X^*)$ the set of all the words which are factors of words in X^*. It is shown in [5] that, for every transitive sofic system $S \subseteq A^Z$, there exists a subset X of A^* such that $L(S) = F(X^*)$. It is easy to verify that one can choose X as a rational subset of A^*. We say that $S \subseteq A^Z$ is a *renewal system* (cf. [11]) if there exists a *finite* subset X of A^* such that $L(S) = F(X^*)$. We also say that the renewal system is *generated* by the set X. In other words, a renewal system is a symbolic dynamical system generated by free concatenations of a finite set of words. Note that all renewal systems are sofic, but that the converse does not hold. Note also that a renewal system is not, in general, of finite type: an example is the renewal system generated by the set $X = \{a^2, b\}$.

Given two systems $S \subseteq A^Z$ and $T \subseteq B^Z$, T is a *factor* of S if there exists a mapping ψ of S onto T which is continuous and commutes with the shift. If ψ is a bijection, S and T are *topologically conjugate*. One of the main open problems of the theory is to decide whether two systems of finite type (or two sofic systems) are topologically conjugate.

The study of renewal systems can play an important role in the conjugacy problem. We consider the following basic questions: (1) Is it decidable whether a sofic system is a renewal system? (2) Is every sofic system topologically conjugate to a renewal system? (3) Is every system of finite type topologically conjugate to a renewal system? (4) Is it decidable whether two renewal systems are topologically conjugate (even under the hypothesis that they are of finite type)?

A positive answer to question 1 has been given by the author in [9]. A negative answer to question 2 has been given by Williams in [11]. Questions 3 and 4 are still unanswered. A positive answer to both these questions would solve the conjugacy problem for the systems of finite type. In this paper we prove the following theorem.

Theorem 1. *Given two systems which are both renewal and Markov systems, it is decidable whether they are topologically conjugate.*

The proof of this theorem is derived by a sequence of results which are interesting in themselves. We need further definitions. A set X of words of A^* is a *code* (cf. [2]) if every word of X^* has a *unique* factorization in elements of X, i.e. if X^* is a *free* submonoid of A^* of base X. A submonoid M of A^* is *very pure* if $uv, vu \in M$ implies $u, v \in M$. It is easy to verify that a very pure submonoid is free. The base of a very pure submonoid is called a *very pure code*. A submonoid $M \subseteq L(S)$ is *S-maximal* if it is

maximal with respect to all submonoids included in $L(S)$, i.e. for any submonoid M', $M \subseteq M' \subseteq L(S)$ implies $M = M'$. The proof of the following theorem in [9] is reported here for completeness sake.

Theorem 2. *For any transitive sofic system S, there exists a finite number of S-maximal submonoids. They are rational sets and can be effectively constructed.*

Proof. Let $\mathscr{A} = (A, Q, q_0)$ be a finite deterministic automaton recognizing $L(S)$. For any subset P of the set of states Q, the *stabilizer* of P is defined as follows:

$$\mathrm{Stab}(P) = \{v \in A^* \mid P.v \subseteq P\}.$$

It is easy to verify that $\mathrm{Stab}(P)$ is a submonoid of A^* and that if $q_0 \in P$, then $\mathrm{Stab}(P) \subseteq L(S)$. Moreover, $\mathrm{Stab}(P)$ is a rational set and a finite automaton $\mathscr{A}(P)$ recognizing it can be constructed as follows. The set of states of $\mathscr{A}(P)$ is the set 2^Q of the subsets of Q. If $V \in 2^Q$ and $a \in A$, the transition function $V.a$ of $\mathscr{A}(P)$ is defined as follows: $V.a = \{q.a \mid q \in V\}$ if $q.a$ is defined for all $q \in V.a$ is not defined otherwise. The initial state of $\mathscr{A}(P)$ is $P \in 2^Q$, and $W \in 2^Q$ is a final state if $W \subseteq P$. We now prove that, for any S-maximal submonoid M, there exists a set $P \subseteq Q$ such that $M = \mathrm{Stab}(P)$. We first prove that for any submonoid $M \subseteq L(S)$ there exists a set $P \subseteq Q$ such that $M \subseteq \mathrm{Stab}(P)$. Set $P = \{q = q_0.v \mid v \in M\}$. For $u \in M$, we have to prove that, for any $q \in P$, $q.u \in P$. Indeed, $q \in P$ implies that there exists $v \in M$ such that $q = q_0.v$. Then $q.u = q_0.vu \in P$ since $vu \in M$. In order to conclude the proof, note that q_0 belongs to P, so that $\mathrm{Stab}(P) \subseteq L(S)$. With M S-maximal, then $M = \mathrm{Stab}(P)$. □

Theorem 3. *Let S be a system of finite type. If S is a renewal system, then there exists an S-maximal submonoid M which is finitely generated. Moreover, $F(M) = L(S)$.*

Proof. If S is a renewal system, there exists a finite set X such that $L(S) = F(X^*)$. Since X^* is a submonoid included in $L(S)$, there exists an S-maximal submonoid M such that $X^* \subseteq M$. We prove that M is finitely generated. Let Z be the minimal generating set of M: $Z^* = M$. Let us suppose, by contradiction, that Z is infinite. Since X is finite, there exists a finite subset Y of Z such that $X \subseteq Y^*$. $X^* \subseteq Y^* \subseteq Z^* \subseteq L(S)$ and $F(X^*) = L(S)$ imply $F(Y^*) = F(Z^*) = L(S)$. Since S is a system of finite type, there exists a finite set H such that $L(S) = A^* - A^*HA^*$. Let k be an integer greater than the maximal length of words in $H \cup Y$, and consider a word $z \in Z$ of length $|z| > 3k$. Since $F(Y^*) = F(Z^*)$, there exist words $s, t \in A^*$ such that

$$szt = y_1 y_2 \ldots y_n, \quad y_i \in Y.$$

By a length argument, there exists a factorization $z = z_1 z_2$ with $|z_1|, |z_2| > k$ and such that z_1 has a suffix of length greater than k in Y^* and z_2 has a prefix of length greater than k in Y^*. One derives that the factors of length k of the words $z_1 z_2$, wz_1, $z_1 w$, wz_2, $z_2 w$, with $w \in Z^*$, do not belong to H. It follows that no word in the submonoid

$M' = (Z \cup \{z_1\} \cup \{z_2\})^*$ has a factor in H. One derives that $Z^* = M \subseteq M' \subseteq L(S)$, against the hypothesis that M is S-maximal. This concludes the proof. □

Using Theorems 2 and 3, one can decide whether a system of finite type is a renewal system. The next theorem provides a sufficient condition for a renewal system to be of finite type.

Theorem 4 (Restivo [8]). *A renewal system generated by a very pure code is of finite type.*

For any finite set $X = \{x_1, x_2, \ldots, x_n\}$ of words, denote by $\lambda(X)$ the *length multiset* of X

$$\lambda(X) = \{|x_1|, |x_2|, \ldots, |x_n|\},$$

where $|x_i|$ is the length of the word x_i $(1 \leqslant i \leqslant n)$.

Theorem 5 (Bertrand-Mathis et al. [3]). *Let S (T) be a renewal system generated by a very pure code X (Y). S and T are topologically conjugate if and only if $\lambda(X) = \lambda(Y)$.*

Theorem 6. *Let S be a Markov system. Every S-maximal submonoid is very pure.*

Proof. Since S is a Markov system, there exists a set $H \subseteq A^2$ such that $L(S) = A^* - A^*HA^*$. Let M be an S-maximal submonoid. Consider two words $u, v \in A^*$ such that $uv, vu \in M$. We prove that $u, v \in M$. In the case where either u or v is the empty word, the statement is trivially true. Consider then the case $u, v \neq 1$. For any word $x \in A^*$, denote by first(x) (last(x)) the first (the last) letter in the word x. For any word $w \in M$, consider the words uw and wu. Since $vuw \in M$ and $wuv \in M$, it follows that last(u)first(w) $\notin H$ and last(w)first(u) $\notin H$. Thus, $uw, vu \in L(S)$. By a similar argument, $uw, wv \in L(S)$. One derives that $(M \cup \{u\} \cup \{v\})^* \subseteq L(S)$. The hypothesis that M is S-maximal implies that $u, v \in M$. This concludes the proof. □

Theorem 6 does not hold if S is not a Markov system, even if it is of finite type, as shown by the following example. Let S be a system of finite type defined by all sequences over the alphabet $\{a, b\}$ which do not contain the occurrence of the factor aba. The submonoid $\{a, b^2, b^3\}^*$ is S-maximal and is not very pure (it is not even free).

Proof of Theorem 1. Given two Markov systems S and T, construct, by using the algorithm in the proof of Theorem 2, all S-maximal and T-maximal submonoids. Since both S and T are renewal systems, by Theorem 3 there exist an S-maximal submonoid M and a T-maximal submonoid M' which are generated by the finite sets X and Y, respectively: $M = X^*$ and $M' = Y^*$. Note that the sets X and Y can be effectively constructed using standard algorithms from automata theory. Note also

that, by Theorem 3, X and Y generate the renewal systems S and T, respectively: $L(S)=F(X^*)$, $L(T)=F(Y^*)$. By Theorem 6, X and Y are very pure codes. Thus, by applying Theorem 5, in order to decide whether S and T are topologically conjugate, there remains to be checked the equality $\lambda(X)=\lambda(Y)$. This concludes the proof. □

References

[1] M.P. Béal, Codes circulaires, automates locaux et entropie, *Theoret. Comput. Sci.* **57** (1988) 283–302.
[2] J. Berstel and D. Perrin, *Theory of Codes* (Academic Press, New York, 1985).
[3] A. Bertrand-Mathis, F. Blanchard and G. Hansel, Sur la fonction ζ de certains systems dynamiques symboliques, preprint, 1987.
[4] F. Blanchard, Codes engendrant certaines systemes sofiques, *Theoret. Comput. Sci.* **68** (1989) 253–265.
[5] F. Blanchard and G. Hansel, Systemes codes, *Theoret. Comput. Sci.* **44** (1986) 17–49.
[6] M. Denker, C. Grillenberger and K. Sigmund, Ergodic theory on compact spaces, Lecture Notes in Mathematics, Vol. 527 (Springer, Berlin, 1976).
[7] S. Eilenberg, *Automata, Languages and Machines* (Academic Press, New York, 1974).
[8] A. Restivo, On a question of McNaughton and Papert, *Inform. and Control* **25** (1974) 93–101.
[9] A. Restivo, Finitely generated sofic systems, *Theoret. Comput. Sci.* **65** (1989) 265–270.
[10] B. Weiss, Subshifts of finite type and sofic systems, *Monatsh. Math.* **77** (1973) 462–474.
[11] S. Williams, Notes on renewal systems, preprint, 1986.